DAS

# Fact Sheet for U.S. Congress H.R. 4127
# Data Accountability and Trust Act (DATA)

The bill applies to "Information Brokers":

H.R. 4127, Section 5(6)

INFORMATION BROKER- The term `information broker' means a commercial entity whose business is to collect, assemble, or maintain personal information concerning individuals who are not customers of such entity for the sale or transmission of such information or the provision of access to such information to any third party, whether such collection, assembly, or maintenance of personal information is performed by the information broker directly, or by contract or subcontract with any other entity.

The underlying DATA Act would:

- Direct the FTC to create rules setting rigorous national standards for data brokers to protect personal information.
- Require data brokers to have a security policy that explains the "collection, use, sale, other dissemination, and security" of the data they hold.
- Require entities to appoint and identify a person in the organization that is responsible for information security.
- Require any entity that experiences a breach of security to notify all those in the United States whose information was acquired by an unauthorized person as a result of the breach. Conspicuous notice on the breached entity's Web site is also required. The FTC must also be notified.
- Provide for an FTC or independent audit of an information broker's security practices following a breach of security. Permit the FTC to conduct or require audits for a period of five years after the breach, or until the commission determines security practices are in compliance with the act and are adequate to prevent further breaches.

The recent manager's amendment would:

- Narrow the definition of data brokers to include only those entities that sell non-customer data to nonaffiliated third parties, ensuring mailing lists and others aren't inadvertently affected by the law. The FTC would also be granted the authority to deem in compliance with H.R. 4127 those companies already meeting the Fair Credit Reporting Act, Gramm-Leach Bliley Act or the Health Insurance Portability and Accountability Act (HIPPA) requirements.
- Require data brokers to establish reasonable procedures to verify the accuracy of information that they collect and maintain.
- Change the threshold for consumer notification from "significant risk of identity theft" to "reasonable risk of identity theft to the individual to whom the personal information relates, fraud or other unlawful conduct."
- Require data brokers to regularly monitor security systems for breaches.

- Prohibit data brokers from obtaining information on someone by impersonating that person - also known as "pretexting."
- Allow consumers annual access to records maintained on them by data brokers as well as the right to have inaccurate information corrected or labeled as disputed.
- Require the FTC to notify the Secretary of Health and Human Services if it determines that a data breach includes individually identifiable health information.
- Afford the FTC the flexibility to recognize future methods or technology to safeguard data, not just today's existing encryption capabilities. Exempts from notification requirements data protected by encryption or other approved methods or technology.
- Allow the FTC one year to promulgate rules required by H.R. 4127.
- Require the FTC to study the maintenance of obsolete paper records containing personal information; the language also authorizes the agency to adopt rules to address any shortcomings in existing law.
- Provide for enforcement of H.R. 4127 by both the FTC and state attorneys general.
- Require a telecommunications carrier, cable operator or other information transmitter that becomes aware of a security breach to report it.

**H.R. 4127 Section 6. Effect on Other Laws**

(a) Preemption of State Information Security Laws- This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly--

(1) requires information security practices and treatment of personal information similar to any of those required under section 2; and

(2) requires notification to individuals of a breach of security resulting in unauthorized acquisition of their personal information.

(b) Additional Preemption-

(1) IN GENERAL- No person other than the Attorney General of a State may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

(2) PROTECTION OF CONSUMER PROTECTION LAWS- This subsection shall not be construed to limit the enforcement of any State consumer protection law by an Attorney General of a State.

(c) Protection of Certain State Laws- This Act shall not be construed to preempt the applicability of--

(1) State trespass, contract, or tort law; or

(2) other State laws to the extent that those laws relate to acts of fraud.